Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities

January 2001

VI. INDUSTRY INTERIM PROGRESS REPORTS

VI. INDUSTRY INTERIM PROGRESS REPORTS

The reports that follow were voluntarily provided by several industry sectors and partnerships, representing a sample of progress and activities within industry over the last year and a half on critical infrastructure protection. The critical infrastructure industries vary widely in their cultures, industry structures, and ways of operating, reflecting and responding to their different market structures, current competitive processes, and regulatory regimes. These reports reflect those differences and at the same time reflect a common business perspective and approach to the issues, starting with a development of an industry business case for action, and including finding the most efficient ways of addressing the issue, such as learning and joining with each other to address common issues and concerns.

This section includes reports from:

Banking and Finance Sector

This joint report by the sector and the Department of Treasury was provided through the Department of Treasury and describes the accomplishments and activities supporting PDD-63 by the banking and finance industry.

Electric Power Sector

The Secretary of Energy asked the North American Electric Reliability Council (NERC) to take on the sector coordinator role for the electric power sector. Because of its long history of providing a forum for electric operations representatives from all parts of the industry to come together to work on reliability issues, it already had an organizational and procedural structure to address the issue of electric infrastructure protection. Its report, originally provided to NERC's Board of Trustees in October 2000, documenting its progress and activities follows.

Oil and Gas Sector

The National Petroleum Council (NPC), a CEO advisory council to the Secretary of Energy, was asked to take on the role of sector coordinator for this industry. It tasked a working group consisting of executive management representatives from a wide range of industry institutions to develop a plan and approach to addressing the concerns addressed in PDD-63. The following report represents the substance of the progress of that task force that was presented to the NPC in the fourth quarter of 2000.

The Partnership for Critical Infrastructure Security (PCIS)

The Partnership provides a forum for cross-sector dialogue. The Coordinating Committee of the Partnership, consisting of representatives from all the active industry sectors, and other founding industry representatives, provided an interim status report on its organizing activities and progress. The Coordinating Committee has also provided as part of their report an interim report from their working group on Policy and Legal Issues that are of particular concern to industry.

Banking And Finance

Introduction

Presidential Decision Directive 63 assigned Treasury "lead agency" responsibility for working with the banking and finance sector of the economy, a responsibility managed by Treasury's Office of Financial Institutions Policy. Treasury Assistant Secretary Gregory Baer serves as Sector Liaison. After consultation with the industry, Treasury named Steve Katz, Chief Information Security Officer of Citigroup, as the industry's Sector Coordinator. Together, Treasury and the industry are responsible for carrying out a number of tasks, including:

- Assessing the vulnerabilities of the sector to cyber and physical attacks;
- Recommending a plan to eliminate significant vulnerabilities;
- Developing an information sharing system for identifying and preventing major attacks;
- Proposing an agenda of research and development for information systems security;
- Developing an education and outreach program to increase awareness of industry infrastructure security risks; and
- Providing content for the industry's contribution to the *National Plan*.

The Banking and Finance Sector

According to the Federal Reserve, at year-end 1999, total credit market assets held by U.S. financial institutions amounted to about $19.6 trillion. The largest institutions by category were commercial banks ($4.6 trillion in assets), insurance companies ($2.4 trillion in assets), mutual funds ($2.3 trillion), pension funds ($1.8 trillion), and thrift institutions ($1.3 trillion); the remaining assets were distributed among finance and mortgage companies, securities brokers and dealers, and various other financial institutions. Banking and finance also includes, and is critically dependent upon, a variety of specialized service organizations such as securities and commodities exchanges, funds transfer networks, payment networks, clearing companies, trust and custody firms, depositories, and messaging systems. These systems are increasingly deployed globally, among institutions, utilities (such as exchanges and clearing entities) and counter-parties.

Moreover, driven by competitive pressures to acquire increasingly sophisticated and costly technology, banking and financial firms have become progressively more dependent on outsourcing certain activities and relying on third-party providers of systems and applications software, as well as technically skilled personnel. Although not members of the banking and finance sector as traditionally defined, the latter firms now have become an indispensable part of the banking and finance infrastructure.

Early studies of banking and finance concluded that this sector is probably better prepared than most other sectors of the U.S. economy to protect itself against cyber and other infrastructure threats. This "preparedness" is largely attributed to the pervasive understanding in the industry that consumer confidence in the safety and reliability of the financial system is absolutely

essential for continued success and to the long legacy of federal regulation of major categories of financial institutions, such as insured depositories and securities brokers and dealers.

The fact remains, however, that the environment evolves, and infrastructure protection measures must evolve in tandem. In the case of banking and finance, a number of major trends have been identified that almost certainly will mean new or altered vulnerabilities, thereby requiring that existing infrastructure protection measures be modified and strengthened and that additional ones be implemented. These trends include:

- *Consolidation*. Ongoing mergers and acquisitions have led to substantial consolidation throughout banking and finance, resulting in greater concentration of assets and fewer sources of support services. This may mean potentially more risk to the financial system in the event of difficulties at individual entities.

- *Globalization*. Financial transactions and activities now routinely "follow the sun," in that they are carried out "24 by 7," at times with little regard for political or national boundaries. The ubiquity of the Internet allows customers, counter-parties, intermediaries, principal institutions, and others to interoperate and intercommunicate on a global basis. More consolidations are cross border and cross cultural, projecting risks and vulnerabilities onto a global stage.

- *Reengineering*. Financial institutions continue to eliminate redundant operations and facilities, simplify systems and processes, and generally to reduce personnel costs. This may increase the risks associated with facility concentration, the use of "off-the-shelf" software, and dissatisfied employees.

- *Decentralized Technology*. Traditional centralized, limited-access computer systems are rapidly being replaced or supplemented by decentralized, open-access systems. This may increase the risk of unauthorized, potentially malevolent access to financial institutions' data and/or control of institutions' computer systems.

- *Alternative Channels*. Financial services increasingly are distributed via channels other than traditional brick and mortar offices. Points of entry into an institution's systems now often include card-activated terminals, wired and cellular telephones, and personal computers, wherever located. This may increase the risk of unauthorized access.

- *Public Infrastructure*. Financial institutions have increased their reliance on public shared data networks to receive and transmit information and funds, and to provide services to consumers. Shared networks are unlikely to be as secure as proprietary or leased, dedicated networks.

- *Interdependencies*. Banking and finance increasingly depends on external service providers, both basic and specialized in nature. Basic services include electrical energy and telecommunications, both being absolutely essential to the provision of financial services. Specialized services include those provided by information and data processing firms, systems and applications software firms, and firms providing sophisticated

information on financial markets worldwide. Denial of service from any of these external service providers may increase vulnerabilities in the banking and finance sector.

Recent Cyber Attacks

The urgency of addressing the issues outlined above is made clear from even a brief accounting of cyber incidents that occurred just this year. For example:

In December, Creditcard.com was the victim of an extortion attempt by a cyber thief accused of hacking into its site and exposing more than 55,000 credit card numbers on the Internet.

In September, Western Union customer information was exposed while the website was undergoing maintenance. Hackers made electronic copies of credit and debit card information of 15,700 customers.

In August, two Kazakhstan men were arrested in London for breaking into Bloomberg L.P.'s New York computer system in an attempt to extort $200,000 from the business news service and its owner.

In May, the "Lovebug" virus was unleashed by an individual residing in Manila, overloading corporate e-mail systems in numerous countries and causing damages estimated at up to $10 billion.

In March, two British teens were arrested for breaking into e-commerce Internet sites in five countries and stealing information from 26,000 credit card accounts.

In February, major U.S. e-commerce sites were disrupted with distributed denial of service attacks, causing over $1.2 billion in damages. Also, a disgruntled Chinese national employee at Deutsch Morgan Grenfell in New York planted a "time bomb" in a computer program that cost DMG $50,000 to fix.

Industry Activities and Accomplishments

As a first step toward the private sector outreach mandated by PDD-63, former Secretary Robert Rubin convened a Treasury information security conference on October 7, 1998. Attendees included a large number of industry information security officers and representatives of the financial regulatory agencies and others with a direct interest in critical infrastructure protection.

Industry representatives at the October 7 conference readily agreed that the goals of PDD 63 were worth pursuing, and they agreed to create and support what is now known as the *Banking and Finance Sector Coordinating Committee on Critical Infrastructure Protection* (the Coordinating Committee), chaired by Sector Coordinator Katz. The industry representatives also established four working groups to address the issue areas they considered to be of highest priority: vulnerability assessment; research and development; education and outreach; and information sharing. This blueprint has defined the activities of the industry since October 1998.

The second meeting of the Coordinating Committee, on March 11, 1999, was a "nuts-and-bolts" type of meeting that established specific agendas for each of the working groups going forward. At that meeting it also was decided that the creation of an industry information sharing and analysis center (ISAC) was especially important, largely because of impending Y2K concerns among government and industry leaders and other signs of an increase in cyber threats. The third meeting, held on April 10, 2000, focused on assessing the vulnerability of the financial services sector to attack and on research and development priorities.

Each of the working groups is at a different stage in their activities. The R&D Working Group is consulting government, academic, and industry experts to develop priorities for government- and private sector-funded research. The Vulnerability Assessment Working Group is reviewing a vulnerability analysis prepared for the President's Commission in 1997, and working on a plan for a follow-up vulnerability assessment of its own. The Outreach Working Group has worked with the Critical Infrastructure Assurance Office at the Commerce Department to help raise awareness of these issues, and is working on a plan for industry education and outreach. The recently established National Plan Steering Committee is drafting the sector's preliminary infrastructure assurance plan and coordinating with the Partnership for Critical Infrastructure Security.

The Financial Services Information Sharing and Analysis Center (FS/ISAC)

One of the most important goals of PDD 63 was the establishment of private sector information sharing and analysis centers (ISACs). These centers would be designed to detect and analyze actual or potential cyber attacks, and distribute alerts about, and suggested remedies for, such attacks to their respective industry sponsors, the actual owners and operators of the critical infrastructures.

The financial services industry was the first to respond to PDD 63's call for the establishment of an ISAC. After an arduous period of technical, legal, and organizational negotiations, approximately a dozen major financial services firms and industry utilities established the Financial Services Information Sharing and Analysis Center – the FS/ISAC. Its official opening was announced by Treasury Secretary Summers on October 1, 1999, with assistance from Chairman Arthur Levitt of the Securities and Exchange Commission, Vice Chairman Roger Ferguson of the Federal Reserve Board, and Richard Clarke of the National Security Council.

The FS/ISAC can be described briefly as follows:

The FS/ISAC is a mechanism for developing and sharing a secure database of information on cyber threats, incidents, vulnerabilities, resolutions and solutions. This information can be shared in an authenticated and anonymous manner, so that member institutions can participate without taking on reputational and other risks.

The FS/ISAC is a limited liability company owned by its members, who include the largest banks, securities firms, insurance companies, and investment companies in the country. The FS/ISAC is not in any way funded or governed by the Treasury Department or any other government agency. Treasury staff attends board meetings solely as observers.

Information comes into the FS/ISAC either from its participating members or from the vendor that operates the center, Global Integrity Corporation, a subsidiary of SAIC. Information contributed to the FS/ISAC can come from publicly available sources, government sources (local, state, and federal), members submitting anonymously, members submitting in an attributable manner, and others. Importantly, no customer account information is shared. No one at Treasury or any other agency sees the input or output of the FS/ISAC.

The sharing of information directly from the government to the FS/ISAC, and eventually from the FS/ISAC to the government and other sector ISACs is under discussion. For example, the FS/ISAC and the Pentagon's Joint Task Force/Computer Network Defense have been discussing such an information sharing agreement; and the FS/ISAC has made it known that it will consider sharing information with other industry ISACs subject to the appropriate protocols.

Participation in the FS/ISAC does not absolve any individual financial institution of its obligation to report criminal activity involving an institution's computer and information systems to the appropriate regulatory and law enforcement authorities.

Although just a year old, the FS/ISAC already has gained notice for outstanding performance during the various denials of service and computer virus attacks of recent months. In Congressional hearings in May, the U.S. General Accounting Office cited the FS/ISAC as the best performing of the various existing public- and private-sector mechanisms intended to provide alerts and countermeasures in defense against information system threats and incidents.

The BITS Financial Services Security Laboratory

Another impressive industry initiative is the financial services security laboratory established in July 1999 by BITS, the technology group for the Financial Services Roundtable, to test products and services that strengthen the security of electronic payments and e-commerce technologies. The goal of the laboratory is to provide the industry and consumers with assurance that financial products have been tested by an unbiased and professional facility and that they meet a prescribed level of security, a fact certified by the issuance of a *BITS Tested Mark*. Like the FS/ISAC, the BITS laboratory is an important, innovative approach to *ex ante* security assurance, and it is another example of the financial sector's commitment to protect providers and users of financial services.

Regulatory and Legislative Initiatives

Several months ago the four Federal depository institution regulators issued a request for comment on a proposed rule establishing standards for safeguarding confidential customer information. Public comments were due this past August 25, and the final rule is now pending. The rule would implement section 501(b) of the *Gramm-Leach-Bliley Act*. Among other things, the rule would provide that financial institutions establish a security program that would require them to: (1) identify and assess the risks that may threaten customer information; (2) develop a written plan containing policies and procedures to manage and control these risks; (3) implement and test the plan; and (4) adjust the plan on a continuing basis to account for changes in

technology, the sensitivity of customer information, and internal or external threats to information security.

In addition, proposed legislation to reduce disincentives to information sharing was introduced in the House earlier this year. The *Cyber Security Information Act* (HR 4246) would encourage the secure disclosure and protected exchange of information about cyber security problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection. It would do this by reducing the risk of antitrust, Freedom of Information Act (FOIA), and liability actions related to cyber security information sharing. Hearings on this bill were held in June, but no further action has been taken. Banking and finance industry representatives intend to address these and other legal issues in the sector's contribution to the *National Plan, version 2*.

Next Steps: Drafting the National Plan

For the immediate future, the banking and finance sector will focus almost exclusively on drafting its contribution to the *National Plan, version 2*. Industry representatives have agreed that topics to be addressed in the sector plan will most probably include information sharing, vulnerability assessment/interdependencies, research and development requirements, education and awareness, sector defense against an attack (continuation of business), reconstitution (how to rebuild after an attack), and legal issues (such as antitrust, FOIA, liability, and privacy).

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

THE ELECTRICITY SECTOR RESPONSE TO

THE CRITICAL INFRASTRUCTURE PROTECTION CHALLENGE
STATUS REPORT AS OF NOVEMBER 2000

The North American Electric Reliability Council (NERC) has been asked on a number of occasions during the past decade to serve as the electric utility industry (Electricity Sector) primary point of contact for issues relating to national security. Since the early 1980s, NERC has been involved with the electromagnetic pulse phenomenon, vulnerability of electric systems to state-sponsored, multi-site sabotage and terrorism, Y2k rollover impacts, and now the threat of cyber terrorism. At the heart of NERC's efforts has been a commitment to work with various federal government agencies to reduce the vulnerability of interconnected electric systems to such threats.

The Report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997 led to a May 1998 Presidential Decision Directive (PDD-63)[1]. PDD-63 called for government agencies to become involved in the process of developing a National Plan for Information Systems Protection, and to seek voluntary participation of private industry to meet common goals for protecting the country's critical systems through public-private partnerships. The PCCIP specifically commended NERC as a model for information sharing, cooperation, and coordination between the private sector and government. In September 1998, Secretary of Energy Bill Richardson wrote to then NERC Chairman Erle Nye seeking NERC's assistance, on behalf of the Electricity Sector, in developing a program for protecting the nation's critical electricity sector infrastructure. Responding to the U.S. Department of

[1] The Presidential Decision Directive 63 (PDD-63) states in part:

> *"No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the signing of Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:*
>
> — *the federal government to perform essential national security missions and to ensure the general public health and safety;*
> — *state and local governments to maintain order and to deliver minimum essential public services;*
> — *the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.*
>
> *Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."*

Energy's (DOE) critical infrastructure protection initiative, NERC agreed to participate as the Electricity Sector coordinator.

As part of this public-private partnership, DOE, the U.S. government's designated Energy Sector Liaison, worked through its Infrastructure Assurance Outreach Program to performed an information assurance assessment for a small number of nodes on NERC's industry information system. The purpose of this assessment was to help NERC and the electric industry develop an overall security framework to address the changing industry structure and the threat of cyber and physical intrusion. A second follow on information system assessment will be performed in late 2000 and early 2001. The product of this study will be recommendations that will form the basis of a draft NERC policy on information assurance. In addition, to facilitate the transfer of information to industry that may be of value in the operation of the electric systems in North America, DOE has provided clearances for several industry personnel and clearances for other key industry personnel are anticipated. These clearances compliment those obtained through another government program, which is discussed below.

Critical Infrastructure Protection Working Group (CIPWG)

After several exploratory scoping sessions with the DOE and the National Infrastructure Protection Center (NIPC), NERC created a Critical Infrastructure Protection (CIP) Forum to evaluate the value of sharing cyber and physical incident data affecting the bulk electric systems in North America. The meetings of this group were widely noticed and the participants included all segments of the electric utility industry and representatives from several government agencies including the Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce, DOE, and NIPC. As a result of their deliberations, NERC created a permanent group within the NERC committee structure. The Critical Infrastructure Protection Working Group (CIPWG) reports to the Operating Committee, with Regional and sector representation and participation by CIAO, DOE, NIPC, American Public Power Association (APPA), Canadian Electricity Association (CEA), Edison Electric Institute (EEI), Electric Power Supply Association (EPSA), Electric Power Research Institute (EPRI), National Rural Electric Cooperative Association (NRECA), and Power Marketers.

Indications, Analysis, and Warnings Program

One of the first tasks of the Forum was to develop the incident data types and event thresholds to be used in an information-sharing program with NIPC. Information sharing (electronic and telephone) mechanisms have been developed for use by electric transmission providers, generation providers, and other industry entities for reporting on a voluntary basis to both NIPC and NERC. Assessments, advisories, and alerts prepared from analyses by NIPC (with NERC's support) based on the data provided by the Electricity Sector (ES) together with data from other sectors, will be stated in an actionable manner and will be transmitted to ES entities. This proposed process was successfully tested within one Region during the fall 1999 and winter 1999–2000. Because of the nature of some of the analyses, government security clearances have been acquired for key industry personnel (three NERC staff members currently hold U.S. clearances) and other industry personnel are in the process of obtaining security clearances.

The Indications, Analysis, and Warnings Program, which evolved from this work, was presented in July 2000 to the Operating Committee. The Operating Committee approved a motion to establish the program in the Electricity Sector (Canada and United States) with initial emphasis on reporting by Security Coordinators and Control Areas. Marketers and the other electric power providers are encouraged to participate by submitting incident data and receiving the various types of NIPC warnings. Workshops were conducted during the fall 2000 to provide program details to the sector.

The Indications, Analysis, and Warnings Program is a voluntary first step toward preparing the Electricity Sector to meet PDD-63 objectives.

Electricity Sector Information Sharing and Analysis Center (ES-ISAC)

The PCCIP recommended that each of the critical sectors establish an Information Sharing and Analysis Center (ISAC) to help protect the infrastructures from disruption arising from coordinated intrusion or attack. The ISACs would gather incident data from within their respective sectors, perform analysis to determine potential malicious intent, share findings with other ISACs (private and government) in a manner that assures, as required, target identity protection and disseminate useful warnings to the personnel identified to take appropriate action within each sector. ISACs would serve as points of contact between sectors to facilitate communications, especially during a time of stress. ISACs would study cross sector interdependencies to better understand and be prepared for the possible impacts of an "outage" of one sector on another.

The CIPWG has endorsed, and NERC has accepted, the naming of NERC as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The functions performed are essentially the same as those functions that have been required of NERC for physical sabotage and terrorism. The ES-ISAC's duties are:

1. Receive voluntarily supplied incident data from ES entities.
2. Work with NIPC during its analysis of incident data to determine threat trends and vulnerabilities.
3. Assist the NIPC personnel during its analyses on a cross private and federal sector basis.
4. Disseminate threat and vulnerability assessments, advisories, and alerts to all those within the ES who are able to take action.

Duties one and four have been assigned to the existing NERC staff. More definition is being established for duties two and three. The ES-ISAC is staffed on workdays with on-call provision for all other periods. Should this capability need to be enhanced, NERC will likely request support for a 24- hour-seven days a week staffed facility.

NERC will establish relationships with the other ISACs as they form.

Critical Infrastructure Protection Planning

The CIPWG, working with CIAO, has written a Business Case for Action to delineate the need for critical infrastructure protection by the ES. Separate papers have been prepared for CEOs, COOs, CIOs, and a NERC general overview. The purpose of the Business Case is to persuade ES participants of the need to report cyber intrusion incidents and to be mindful of the possible business losses caused by cyber and physical intrusion.

The CIPWG is developing what may become a basic and fairly comprehensive plan to address the CIP issues in the ES. The Working Group is concerned about generating an overly prescriptive plan too early in the process and is proceeding with a format that can assist in developing each entity's own plan. The prototype plan addresses awareness, threat and vulnerability assessment, practices that can be considered, risk management schema, reconstitution, and interdependencies between and among sectors.

The essence of this "Approach to Action" will be considered for inclusion in Version 2.0 of the National Plan for Information Systems Protection being compiled by the U.S. Government. Richard Clarke,

Special Assistant to the President and National Coordinator for Security, Infrastructure Protection, and Counter-terrorism, recently discussed the importance of establishing and maintaining a National Plan to the health of the government and private sectors, companies, and the nation. Version 1.0 of the Plan did a good job covering the threats and the government response, but it did not detail private sector response. The need for private sector participation is engendered by the fact that the government lacks private sector expertise and needs private sector "buy in" to CIP initiatives. The National Plan version 2.0, which will include private sector input, is scheduled for spring 2001.

Partnership for Critical Infrastructure Security (PCIS)

The Partnership for Critical Infrastructure Security was proposed in late 1999 by members of several private sectors; the PCIS is supported by CIAO and the U.S. Chamber of Commerce. The PCIS Mission:

> Coordinate cross-sector initiatives and complement public/private efforts to promote and assure reliable provision of critical infrastructure services in the face of emerging risks to economic and national security.

The PCIS held two general forums in 2000 and is planning two general forums in 2001 — March 20–21 and September 6–7. The PCIS has formed six active working groups: Interdependency Vulnerability Assessment and Risk Management; Information Sharing, Outreach and Awareness; Public Policy and Legislation; Research and Development and Workforce Development; Organization Issues and Public-Private Relations; and National Plan.

NERC is participating in the PCIS. The opportunities presented by PCIS include gaining a better perspective of the sector interdependencies, facilitating ISAC formation, and sharing of common research and development efforts.

NATIONAL PETROLEUM COUNCIL

COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

Progress Report to the
National Petroleum Council

January 10, 2001

The National Petroleum Council began its study on Critical Infrastructure Protection in late 1999 in response to a request from Secretary of Energy Bill Richardson. The Secretary asked the Council to provide advice on cooperative approaches to protecting the critical infrastructure of the oil and gas industry. The Secretary's letter states:

> The Federal Government is aggressively pursuing a variety of approaches through which the critical infrastructures of the United States can be protected from physical and cyber threats. To be effective, however, these approaches must be developed and implemented in partnership with the industry because the private sector owns and controls the vast majority of the Nation's critical infrastructures.
>
> Accordingly, I request the National Petroleum Council to review the potential vulnerabilities of the oil and gas industries to attack--both physical and cyber--and to advise me on policies and practices that industry and Government, separately and in partnership, should adopt to protect or recover from such attacks.

(The complete text of the Secretary's request letter is attached.)

SCOPE OF WORK

At the outset, the Council developed the following broad scope of work to focus and guide its study efforts:

- Develop a thorough understanding of the emerging overall federal program on Critical Infrastructure Protection and coordinate with other sectors (electric, telecommunications, transportation, finance, etc.) to benefit from their experience and analyses.

- Develop the Business Case for proceeding with discussion of "Cooperative Approaches" with industry and/or government.

- Define asset criticality and security risk in the context of Critical Infrastructure Protection for the oil and gas sector.

- Assess the vulnerabilities of the oil and gas sector to cyber and physical attacks. The assessment is to be a generic overview of potential vulnerabilities based on threat capabilities.

- Develop potential policies and practices that industry and government, separately and in partnership, should adopt to protect or recover from such attacks. This includes evaluating potential risk assessment models suitable for the oil and gas sector.

- Propose mechanisms through which industry can beneficially access relevant federal law enforcement and intelligence assets.

- Assess and make a recommendation concerning the need for an "Information Sharing and Analysis Center" for the oil and gas sector, similar to those that currently exist for safety.

- Study liability and legal impediments to information sharing and other concerns such as protection of confidential and proprietary information.

- Outline potential research and development requirements to enhance Critical Infrastructure Protection.

ORGANIZATION

With Secretary Richardson's approval, the Council established a Committee on Critical Infrastructure Protection to prepare a response to his request. The Committee is assisted by a Coordinating Subcommittee, which is evaluating the issues raised by the Secretary and is developing for the Committee's consideration, recommendations for alternative courses of action. (The Secretary's approval letter and the rosters of the Committee on Critical Infrastructure Protection and its Coordinating Subcommittee are attached.)

To facilitate the completion of its work, the Subcommittee has organized itself into a series of informal work groups. These groups are responsible for returning to the whole Subcommittee proposed report sections in the following assigned areas:

- Vulnerability Assessment and Reduction Measures

- Information Sharing and Analysis

- Federal CIP Program Coordination

- Legal and Liability Issues

The work groups meet as needed and the Subcommittee tracks overall progress at 30-60 day intervals. In addition, several "information sessions" have been held where all subcommittee members are given the opportunity to be briefed on the CIP activities of other industries as well as the emergency preparedness and response and recovery programs of the various federal and local agencies that may have a role.

The Department of Energy and the National Laboratories are providing significant technical and logistical support to the subcommittee and each subgroup. Additional federal support is being provided by the Departments of Commerce, Justice, Defense, and Transportation.

CURRENT STATUS

The Subcommittee has completed the basic research phase of its work and has begun analyzing this information in the context of the current realities of the global oil and gas Industry. The research has covered the plans and programs of the following government and industry groups.

Federal Level

- Office of the President
  - Presidential Commission on Critical Infrastructure Protection
  - Presidential Decision Directives 39, 62, and 63
- Department of Commerce
  - Critical Infrastructure Assurance Office
  - Partnership for Critical Infrastructure Security
- Department of Justice
  - FBI
    - -- National Infrastructure Protection Center
    - -- InfraGuard
    - -- Key Asset Program
  - Antitrust Division
- Department of Energy
  - Lead PDD 63 Agency for Electric Power, Oil, and Natural Gas
  - National Labs and Research Programs
- Department of Defense
  - Defense Information Systems Agency
  - U.S. Army
    - -- Director of Military Support
    - -- Corps of Engineers
- Department of Transportation
  - Office of Pipeline Safety
  - Coast Guard

Federal Level (Continued)

- Federal Emergency Management Agency
- Environment Protection Agency

State Level

- National Association of State Energy Officials
- New York State Energy Research and Development Authority

Local Level

- Harris County, Texas
  - -- Houston TranStar

Critical Industries and Their Information Sharing Approaches

- Electric Power – North American Electric Reliability Council
- Telecommunications – National Security Telecommunications Advisory Council
- Information Technology - Information Technology Association of America; World Information Technology Services Alliance
- Banking and Finance - Financial Services Information Sharing and Analysis Center; Banking Industry Technology Secretariat

The Subcommittee is now focusing on four major remaining areas of study:

- Legal implications of attacks and preventative and restorative measures for companies, shareholders, and employees
- Structure and operating principles for information sharing in the oil and gas industries including identification of proposed support contractor
- Role and identification factors of permanent sector coordinator for the oil and gas industries
- Overall report recommendations to government and industry.

The final attachment is the Subcommittee's current report outline. The various work groups have been assigned specific chapters and have developed initial drafts. Final drafting is being conducted concurrently with the work on the four remaining study areas. Both efforts will be brought together in the January-March timeframe in the form of the Subcommittee's consolidated draft of the overall study report.

TIMETABLE

Secretary Richardson's request of the Council fits into an overall governmental program that calls for critical infrastructure protection programs to reach "initial" operating capability in year 2000 and full capability no later than 2003. The following study timetable is consistent with that guidance:

December 1999	Scope of work approved and Coordinating Subcommittee staffed
January-June 2000	Subcommittee begins basic research and determines form of final report
June	Report progress and plans to Committee and Council
July December	Continue subgroup work and begin Subcommittee delib erations on consolidated report
January-March 2001	Complete Subcommittee analyses and finalize proposed recommendations and draft report
April-May	Subcommittee forwards its final draft report to the Committee, which then meets to review and comment
May-June	Committee forwards proposed final report to Council, which then meets to consider it as proposed response to Secretary of Energy's request. The date of this meeting tentatively has been set for June 6, 2001.

The Secretary of Energy
Washington, DC 20585

April 7, 1999

Mr. Joe B: Foster
Chair
National Petroleum Council
1625 K Street, N.W.
Washington, D.C. 20006

Dear Mr. Foster:

Thank you for your letter of December 14, 1998. I am writing to formally request the Council's advice on cooperative approaches to protecting the critical infrastructure of the United States oil and gas industry.

The Federal Government is aggressively pursuing a variety of approaches through which the critical infrastructures of the United States can be protected from physical and cyber threats. To be effective, however, these approaches must be developed and implemented in partnership with the industry because the private sector owns and controls the vast majority of the Nation's critical infrastructures. You have indicated that the Council believes it can contribute meaningfully to these efforts and can provide advice on a systematic approach to the planning process for protecting the critical infrastructures of the oil and gas industry.

Accordingly, I request the National Petroleum Council to review the potential vulnerabilities of the oil and gas industries to attack--both physical and cyber--and to advise me on policies and practices that industry and Government, separately and in partnership, should adopt to protect or recover from such attacks.

Specifically, I would like the Council to advise me on:

1. definitions of criticality and risk in the context of critical infrastructure protection of oil and gas system infrastructures;

2. remedies for legal concerns such as protection of confidential information and the ability of competing firms to participate in cooperative relationships, and

3. mechanisms through which the industry car, beneficially access relevant Federal law enforcement and intelligence assets and through which industry can both benefit from and help prioritize Government research and development programs in infrastructure assurance.

Finally, Presidential Decision Directive 63, which implements the recommendation of the President's Commission on Critical Infrastructure Protection, calls for me to designate a Sector Coordinator for the oil and gas industry. For the duration of your study, I would like the National Petroleum Council to take on the responsibility of the Sector Coordinator. At the conclusion of 'your work, I would like your advice on the permanent role of the Sector Coordinator and your recommendation on how that person or organization should be identified. The North American Electric Reliability Council has been designated as the Sector Coordinator for the electric industry and. to recognition of the growing interrelationship between the gas and electric industries. you should collaborate with that group as appropriate. Further, the Departments of Transportation and Energy have agreed to share critical infrastructure protection responsibilities for the Nation's oil and gas pipeline systems. Your advice, therefore, should consider oil and gas infrastructures from production to consumption.

Given the nature of this request, Under Secretary Emest J. Moniz will represent the Department and will provide appropriate coordination with the Department of Transportation and other branches of Government.

As always I appreciate the Council's ongoing assistance in these issues of national policy and mutual concern.

Yours sincerely,

Bill Richardson

Cc: Richard Clark
Rodney E. Slater
Erle Nye
Michehl Gent

The Secretary of Energy
Washington, DC 20585

October 15, 1999

Mr. Joe B: Foster
Chair
National Petroleum Council
1625 K Street, N.W.
Washington, D.C. 20006-1656

Dear Mr. Foster:

This letter conveys my approval to establish a Committee on Critical Infrastructure Protection and to appoint the members of the Committee as proposed in your letter of August 9, 1999.

The Government Co-chair for the Committee will be retired Air Force General Eugene E. Habiger, Director of the recently established Office of Security and Emergency Operations. The Office of Fossil Energy has substantial interest in this topic and will continue to work cooperatively with the Office of Security and Emergency Operations to address critical infrastructure issues related to the electricity, oil and gas industries.

I am pleased that the National Petroleum Council has accepted responsibility for reviewing the potential vulnerabilities of our Nation's oil and gas critical infrastructure and advising me on policies and practices that Government and industry, separately and in partnership, should adopt to ensure its integrity. The Council's willingness to additionally serve as the interim Sector Coordinator for the oil and gas Industry for the duration of your study is deeply appreciated.

Yours sincerely,

Bill Richardson

Bill Richardson

NATIONAL PETROLEUM COUNCIL

COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

CHAIR
David J. Lesar
Chairman of the Board, President
and Chief Executive Officer
Halliburton Company

GOVERNMENT COCHAIR
Eugene E. Habiger
Director
Office of Security and
Emergency Operations
U.S. Department of Energy

EX OFFICIO
Archie W. Dunham
Chair
National Petroleum Council

EX OFFICIO
William A. Wise
Vice Chair
National Petroleum Council

SECRETARY

Marshall W. Nichols
Executive Director
National Petroleum Council

* * *

Riley P. Bechtel
Chairman and
Chief Executive Officer Bechtel
Group, Inc.

David W. Biegler
President and
Chief Operating Officer
TXU

Peter I. Bijur
Chairman of the Board and
Chief Executive Officer
Texaco Inc

M. Frank Bishop
Executive Director
National Association of
State Energy Officials

Philip J. Carroll
Chairman and
Chief Executive Officer
Fluor Corporation

R. D. Cash
Chairman, President and
Chief Executive Officer
Questar Corporation

Robert B. Catell
Chairman and
Chief Executive Officer
KeySpan Energy

Hector J. Cuellar
Managing Director
Area/Industries Manager
Bank of America

Ronald A. Erickson
Chief Executive Officer
Holiday Companies

Ray L. Hunt
Chairman of the Board
Hunt Oil Company

Kenneth L. Lay
Chairman and
Chief Executive Officer
Enron Corp.

NPC COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

David L. Lemmon
President and
Chief Executive Officer
Colonial Pipeline Company

John H. Lichtblau
Chairman and
Chief Executive Officer
Petroleum Industry Research
Foundation, Inc.

Steven L. Miller
Chairman, President and
Chief Executive Officer
Shell Oil Company

James J. Mulva
President and
Chief Executive Officer
Phillips Petroleum Company

Richard B. Priory
Chairman and
Chief Executive Officer
Duke Energy Corporation

Daniel Rappaport
Chairman of the Board
New York Mercantile Exchange

Lee R. Raymond
Chairman, President and
Chief Executive Officer
Exxon Mobil Corporation

Richard E. Terry
Chairman and
Chief Executive Officer
Peoples Energy Corporation

Gerald Torres
Associate Dean for Academic Affairs
University of Texas School of Law and
Vice Provost
University of Texas at Austin

C. L. Watson
Chairman of the Board and
Chief Executive Officer
Dynegy Inc.

Daniel H. Yergin
President
Cambridge Energy Research Associates

NATIONAL PETROLEUM COUNCIL

COORDINATING SUBCOMMITTEE
OF THE
NPC COMMITTEE ON
CRITICAL INFRASTRUCTURE PROTECTION

CHAIR

Charles E. Dominy
Vice President
Government Affairs
Halliburton Company

GOVERNMENT COCHAIR

Paula L. Scalingi
Director
Office of Critical Infrastructure Protection
U.S. Department of Energy

ASSISTANT TO THE CHAIR

Forrest L. Carpenter
Manager
Computer Security and
Business Continuity Planning Global
Information Services Texaco Inc.

SECRETARY

Marshall W. Nichols
Executive Director
National Petroleum Council

* * *

Raymond W. Bergeron
Manager
Corporate Security
Shell Oil Company

M. Frank Bishop
Executive Director
National Association of
State Energy Officials

Thomas D. Carmel
Corporate Counsel
Conoco Inc.

Donald M. Field
Executive Vice President
Peoples Energy Corporation

Bobby R. Gillham
Manager Global Security
Conoco Leadership Center
Conoco Inc.

Lawrence J. Goldstein
President
Petroleum Industry Research
Foundation, Inc.

Michael C. Hicks
Manager
Security
Enron Property & Services Corp.

Thomas R. Holland, Jr.
Manager
Corporate Security – Worldwide
Phillips Petroleum Company

Harry Kremling
Managing Director ans
Client Manger
Engineering and Construction Sector
Banc of America Securities LLC

Kevin J. Lindemer
Senior Director
Refined Products
and Global Downstream
Cambridge Energy Research Associates

COORDINATING SUBCOMMITTEE OF THE NPC COMMITTEE ON CRITICAL INFRASTRUCTURE PROTECTION

David J. Manning
Senior Vice President
Corporate Affairs
KeySpan Energy

James R. Metzger
Vice President and
Chief Technology Officer
Texaco Inc.

Rolando D. Moss
Senior Director
Corporate Security
Dynegy Inc.

A. R. Mullinax
Senior Vice President
Global Sourcing and Logistics
Duke Energy Corporation

Frank B. Sprow
Vice President
Safety, Health & Environment
Exxon Mobil Corporation

Catherine A. Travis
Director
Information Security
Questar Corp.

Vic A. Yarborough
Vice President Technology
Colonial Pipeline Company

SPECIAL ASSISTANTS

W. R. Finger
President
ProxPro, Inc.

Ronald E. Fisher
Deputy Director
Infrastructure Assurance Center
Argonne National Laboratory

Joseph A. Gurga
Manager
Program Office
Information Technology Services
Peoples Energy Corporation

John R. Johnson
Principal Advisor
Shell Services International

Stuart L. Schertz
Senior Security Representative
Corporate Security
Shell Oil Company

Curtis R. Smith
Manager
Information Security
Conoco Inc.

Richard D. Vance
Strategic Business Consultant
Duke Energy Corporation

Peter van de Gohm
Director
Information Assets Protection
Enron Energy Services

National Petroleum Council

Securing the Energy Industry in the New Economy

Draft Report Outline of the NPC Committee on Critical Infrastructure Protection

---

I. PREFACE

II. EXECUTIVE SUMMARY

III. FINDINGS AND RECOMMENDATIONS

IV. CHAPTERS

Chapter 1. Purpose and Objectives.

A. Blueprint for Action (strategy document "go forward" view) Brief Discussion of "New Economy" and IT Revolution.

B. Motivation (why committee was commissioned - list members in appendix).

1. Assure Security and Business Continuity of Industry to Meet New Challenges.

2. Raise Level of Awareness and Understanding Within Industry and Government.

3. Identify Necessary Actions and Recommend Appropriate Implementation Steps

Chapter 2. Background.

A. Chapter Summary.

B. Energy Industry Characterization (description, structure of oil and gas industry, dependence on information technology, energy industry interconnectedness [including electric power], interdependencies with other infrastructures [telecommunications, transportation, etc.]).

C. Description of Evolving Energy Industry (market dynamics, diversification, financial posture, new customers, non-traditional competitors, new retail outlets, etc.).

Chapter 2. Background (continued):

D. Importance to Overall Economy, Quality of Life, Human Health and Safety, National Security.

E. New Challenges of the 21st Century.

1. Impacts of New Economy (internal to energy industry, external).
    a. Increased Reliance on E-Commerce and Electronic Markets.
    b. Globalization.
        1. Increase of Foreign Partnership / Ownership
        2. Socio-Economic and Political Impacts.
    c. Interdependencies (growth in electric power usage, ownership of joint infrastructures, joint vulnerabilities [common corridor]).
    d. Workforce (retention, new skill requirements, training and awareness).

2. Restructuring.
    a. Supply / Demand (natural gas as future energy of choice).
    b. New Industry Participants (marketers).
    c. Convergence of Energy Enterprise (providers, markets, systems).
    d. Deregulation of Energy Industry
    e. Lower R&D Budgets

3. Other Major Trends.
    a. Increased Utilization of Assets (JIT) Reduces Spare Capacity.
    b. Reduced Flexibility (rerouting, maintenance).
    c. Lack of Incentives for Capital Expenditures for Infrastructure Upgrades).
    d. Pipeline Maintenance and Vintage.
    e. Environmental Mandates and Barriers (can't get permits).
    f. Increase in Petroleum Imports.

F. Critical Infrastructure Protection

1. New and Broader Threat Environment and Risks
2. Public Perspectives.
3. National/ Industry Perspectives.
4. International Perspectives

Chapter 2. Background (continued):

G. Opportunity to Leverage Y2K Experience (established relationships, organizational structure, IT reliance).

1. Baseline of Information, Response, and Recovery Plans.

2. Set Up Mechanisms for Information Sharing Industry Wide.

3. Preserve and Sustain the Emergency Management Capabilities.

Chapter 3. Threats.

(Objective: gain a sound understanding of industry threats.)

A. Chapter Summary.

B. Threat Environment *(cascading disruptions to infrastructures*).

1. Information Technology based threats.

2. Physical or "Traditional" threats.

3. Natural threats.

4. Regulatory and Restructuring threats.

5. Man-made threats.

6. Interdependency threats.

C. Strategy for Developing Best Practice Methodologies, as appropriate.

Chapter 4. Vulnerabilities.

(Objective: gain a sound understanding of industry vulnerabilities.)

A. Chapter Summary.

B. Definitions of Key Terms and Industry /Government Perspectives.

C. High-Level Overview of Vulnerabilities in the Oil and Gas Sector.

D. Characterization of Criticality of Infrastructure Components from Stakeholders' Perspective (company, industry, public, government).

E. Characterization of Current Assessment Practices and Methodologies.

F. Strategy for Developing Best Practice Methodologies, as appropriate

Chapter 5. Risk Management (including mitigation).
(Objective: gain an understanding of risk management in the new economy, develop a strategy for identifying and producing best practices and methodologies, and build a business case for industry acceptance.)

A. Chapter Summary.

B. How/Why Risks are Different, Methods to Measure Risk and Risk Evaluation.

C. Characterization of Criticality of Infrastructure Components from Stakeholders' Perspective (company, industry, public, government).

1. Critical Assets (definitions, perspectives, prioritization)

D. Strategy for Developing Best Practice Methodologies, as appropriate.

1. Characterization of Current Assessment Practices and Methodologies.

2. Survey Existing Models (insurance industry, audit, accounting standards).

E. Resource Allocation To Mitigate Risks.

F. Relevant Issues.

1. Liability /Indemnification (open-ended liability, industry as target.

2. Funding.

3. Public/ Shareholder Perceptions.

Chapter 6. Response and Recovery.
(Objective: evaluate the need for enhancing response and recovery plans and procedures to meet the challenges of the new economy at the regional, national, and international level.)

A. Chapter Summary.

B. Current State of Response and Recovery Plans and Procedures Including Informal Agreements.

C. Incorporate Lessons Learned From Y2K Contingency Planning into Response and Recovery Planning.

D. Evaluate Optimal Models, e.g., Oil Spill, MMS, CDC, NRC, FEMA, IEA.

E. Gaps and Recommend Additional Enhancements.

F. Best Practices.

G. Periodic Tests (benchmarks, table tops, communications).

Chapter 6. Response and Recovery (continued):

A. Technologies and Methods.

B. Discussion of Roles/Responsibilities/Coordination/Jurisdiction/Cooperation.

1. Industry.
2. Local.
3. State.
4. Federal.
5. Public.
6. International Entities.

Chapter 7. Information Sharing.

(Objective: determine to what extent information should be shared and how.)

A. Chapter Summary.

B. What are the Drivers for Sharing Information?

C. What Information Does Industry Need to Meet the Needs of the New Economy?

D. What are Some of the Barriers to Sharing Information?

E. Ways Information is Currently Shared in Industry-Formal and Informal.

F. Ways Information is Currently Shared between Industry and Government - Formal and Informal.

G. Emerging Models for Information Sharing (Banking & Finance, NSTAC, etc.).

H. Classification Issues/ Confidentiality Agreements.

I. Outline Requirements for the Oil and Gas Sector.

J. Address Foreign Ownership or Controlling Interests.

Chapter 8. Legal and Regulatory Issues.

(Objective: discussion of barriers, incentives, and actions required.)

A. Chapter Summary.

B. Identification of Barriers.

C. Standards (Are they useful or necessary?)

Chapter 8. Legal and Regulatory Issues. (continued):

A. FOIA and Other Information Sharing Issues

1. Anti-Trust.

2. Corrupt Practices Act.

3. Lobbying Disclosure Act.

4. Foreign Agents Registration Act.

5. Privacy Act.

B. Government (federal, state, and local).

Chapter 9. Research and Development Needs.
(Objective: identify gaps, and appropriate roles for industry and government in meeting R&D needs)

A. Chapter Summary.

B. Outline a Strategy For a Needs Assessment Based on Vulnerabilities and Risk Management.

C. How to Accomplish and Keep Current.

1. Industry Roles and Missions.

a. Technology Transfer from Industry to Government.

2. Government Roles and Missions.

a. Technology Transfer from the Government to Industry.

V. APPENDICES

A. Request Letter.

B. Study Rosters.

C. ,etc. (to be developed).

December 10, 2000

Mr. Richard A. Clarke
National Coordinator, Security, Critical Infrastructure Protection, and Counter-Terrorism
National Security Council
The White House
Washington, DC 20504

Dear Mr. Clarke,

The Coordinating Committee of the Partnership for Critical Infrastructure Security is pleased to provide you this status report of its significant activities in the area of critical infrastructure assurance. We trust that this will help in your planning with the transition to a new Administration, and we pledge our support. Please feel free to call on any Coordinating Committee member for additional information or planning assistance.

On behalf of the Coordinating Committee,

Kenneth C. Watson
Cisco Systems, Inc.

Attachments:
Coordinating Committee Members
Status Report

Attachment 1. Coordinating Committee Members

William G. Bishop, III
The Institute of Internal Auditors, Incorporated

Matthew Flanigan
Telecommunications Industry Association

Richard Holmes
Union Pacific Corporation

Jeffrey M. Jaffe
Lucent Technologies

Stephen C. Jordan
U.S. Chamber of Commerce

Stephen R. Katz
Citigroup

Lou Leffler
North American Electric Reliability Council

Harris Miller
Information Technology Association of America

Roy Neel
United StatesTelephone Assocation

Marshall W. Nichols
National Petroleum Council

Richard J. Perlot
SBC Communications, Incorporated

Louis L. Rana
Consolidated Edison Company of New York, Incorporated

Ty R. Sagalow
American International Group, Incorporated

Howard A. Schmidt
Microsoft Corporation

Diane VanDe Hei
Association of Metropolitan Water Agencies

Kenneth C. Watson
Cisco Systems, Inc.

Nancy Wilson
American Association of Railroads

Robert E. Wright
BellSouth

William G. Bishop, III
THE INSTITUTE OF INTERNAL AUDITORS, INCORPORATED

Richard Holmes
UNION PACIFIC CORPORATION

Jeffrey M. Jaffe
LUCENT TECHNOLOGIES

Stephen C. Jordan
U.S. CHAMBER OF COMMERCE

Stephen R. Katz
CITIGROUP

Richard J. Perlot
SBC COMMUNICATIONS, INCORPORATED

Louis L. Rana
CONSOLIDATED EDISON OF NEW YORK, INCORPORATED

Ty R. Sagalow
AMERICAN INTERNATIONAL GROUP, INCORPORATED

Howard A. Schmidt
MICROSOFT CORPORATION

Kenneth C. Watson
CISCO SYSTEMS, INCORPORATED

Robert E. Wright
BELLSOUTH CORPORATION

Partnership for Critical Infrastructure Protection Status Report: November 2000

We, the Coordinating Committee of the Partnership for Critical Infrastructure Security, strongly believe that protecting America's critical infrastructures is and will remain an extremely significant economic and national security issue, requiring coordinated, focused, diligent effort by both the private sector and the Federal Government. Just as with the Year 2000 turnover effort, a coordinated public-private partnership, supported at the highest levels of government and industry, will help promote the actions necessary to preserve our economic and national security. Unlike Y2K, however, this threat and concomitant risk are very difficult to quantify, and there is no given end date against which to plan.

Federal Government Perspective

The US Government has approached industry for help in developing coordinated solutions to counter emerging national security threats. Malicious attacks can come from hackers inside and outside the United States or organized and funded information warriors from potentially hostile foreign governments or extra-national organizations. Unlike traditional threats, in the case of cyber attack, the national security apparatus has little ownership or control of the networks, no jurisdiction in the case of foreign threats, limited intelligence on threats and vulnerabilities, and insufficient research and development capability to develop countermeasures.

US Industry's Perspective

Businesses are just as dependent on electronic information systems and the emerging Internet capabilities for their survival, and work zealously to protect and defend their interests. The same vulnerabilities that threaten national security also threaten economic survivability and competitiveness. Additionally, the infrastructures are themselves interdependent. Banks depend on telecommunications for electronic transactions. Telecommunications companies must have electric power to operate. In turn, much of our electric grid depends on telecommunications. In the United States, individual companies and sectors have begun to address vulnerabilities and develop countermeasures, but the significant interdependencies and the national security component mandate a more coordinated approach.

Public-Private Partnership: The New "Civil Defense"

In close coordination with the Department of Commerce, we launched the PCIS on December 8, 1999, dedicating our efforts to assuring the delivery of essential services over the nation's critical infrastructures. We subsequently organized the PCIS into issue-oriented working groups, and we are collaborating with the Federal Government to write the first-ever coordinated public-private national plan. The PCIS represents a cross-sector industry partnership, but with federal, state, and local government participants, to better address issues of common concern.

The PCIS followed its kick-off meeting with a planning retreat February 22, 2000 in Washington DC, establishing initial working groups and plans. Industry responded enthusiastically. Key companies volunteered to chair the working groups and an ad hoc planning committee, and most participants devoted many hours to working group efforts, hammering out issues for resolution, courses of action, and recommendations for industry. The three major functions established for the PCIS were:

- to provide a mechanism for cross-sector coordination and dialog on critical infrastructure security issues, within industry and with government;
- to facilitate and coordinate cross-sector industry input into subsequent versions of the National Plan; and
- to provide a means to contribute to appropriate government advisory bodies.

The PCIS ad hoc planning committee established the following Working Groups:

- Working Group #1: Interdependency Vulnerability Assessment and Risk Management
- Working Group #2: Information Sharing, Awareness, and Outreach
- Working Group #3: Public Policy and Legislation
- Working Group #4: R&D and Workforce Development
- Working Group #5: Organization Issues and Public-Private Relationships

On July 25-27, 2000, the PCIS met in San Francisco to review the past six months' work, make critical decisions regarding formal organization, and outline the work plan for the next six months. Sector Coordinators, as identified PDD-63, established the PCIS Coordinating Committee as its governing body and identified tasks to:

- move toward a legal, formal organization;
- prioritize the tasks for PCIS Working Groups;
- make membership and support decisions;
- establish a National Plan Working Group (NPWG); and
- continue to make use of the services of the CIAO and US Chamber of Commerce as joint secretariat for the PCIS.

The 162 attendees represented key companies from all critical US infrastructure industries, US federal, state, and local governments, Canada, and Switzerland. Working Group reports illustrated significant work accomplished and outlined an aggressive plan for the next six months. The next meeting is scheduled for March 20-21, 2001 in Washington, DC.

Next Steps

Recognizing that some infrastructures were already at work on single-sector issues involving both government and industry, the Coordinating Committee established the following operating principles to ensure added value to the sectors:

- Build on and complement work of the critical infrastructure sectors identified in PDD-63;
- Support efficiency and add value to ongoing work by identifying and addressing critical common and shared issues across sectors;
- Take on only those initiatives that complement and provide additional efficiencies for the sectors or that otherwise cannot or will not be done; and
- Act as a catalyst for action for existing entities whenever possible.

The PCIS prioritized seven key issue areas meriting priority of effort over the next several months.

1. The next version of the National Plan for Information Systems Protection. The US Government recognized the limitations of its first version as government only, limited to the cyber dimension, and lacking an international perspective. By engaging industry, the next version will address public and private efforts, include both cyber and physical dimensions of protection, and incorporate international issues. The next version of the plan is intended to include input from all 13 Federal key agencies, the 8 critical infrastructure sectors, PCIS working groups, and state and local fire, law enforcement, and emergency services organizations.

2. Interdependency. One area the PCIS can address more easily than a single sector is interdependency risk assessment and management. Industry Sector Coordinators universally endorsed this as the second-most important task to be completed. PCIS Working Group #1 completed a "lessons-learned" study from the Y2K turnover effort and presented its results in July. It also began to identify the information needed to begin a useful study of interdependencies between sectors. It set a work plan to expand its sources of information on interdependency work that has already been done, to define a proposal for a real-world business simulation that will include all critical infrastructure sectors, and to identify a business case for developing a common interdependency risk assessment approach across sectors.

3. Inclusion of state and local governments. To date, the PCIS has had only limited representation from state and local governments. In local communities, private industry has a long history and comfort level in working with state and local governments on various critical service assurance issues. Since state and local governments also make up most of the emergency services first responders and perform the critical coordinating function in local areas for both industry and government, the PCIS is organizing outreach to the National Association of State Information Resource Executives, National Council of Mayors, National Governors' Association, and other groups. We are also encouraging businesses to join state and local chapters of the National Infrastructure Protection Center's InfraGard program.

4. Legislative and regulatory issues. Working Group #3 developed and presented a public policy white paper, "Legal Challenges for Cyber Security Cooperation", to the Partnership in July. It examines legal issues and challenges associated with cyber security risk management issues, some of the challenges seen as legal impediments to industry and cross-sector cooperation, and some of the legal risks that may undermine common sense strategies and prudent risk management activities. In addition, the group sponsored a web cast on the subjects of the white paper to garner more input and explore the issues with a wider range of participants. The group has identified specific issues on which they will explore in greater detail through white papers to be developed as part of their work plan for March 2001. Specific issues that the group will follow up on include: FOIA, antitrust, liability, state of Congressional response to issues acting as impediments to intra- and inter-sector cooperation, and international dialogue and status of cooperation. To support research needed to develop its papers, the group has developed a cooperative relationship with a local university.

5. Awareness. Building awareness and a case for action within industry and government emerges as the foundation for involvement and program implementation for all PCIS working groups, as well as a broad infrastructure security need. This issue is so complex and so basic to society that services delivered over the critical infrastructures are often taken for granted. The Partnership recognized that an intensive six-month program of conferences for chief auditors, Boards of Directors, and other executive corporate officers reached its critical audiences. However, we believe much more is needed. In July, Working Group #2 developed and presented an analysis of Critical Infrastructure Protection awareness program activities. This study resulted in a roadmap of awareness program goals and identified key audience groups. It provided a matrix of current cross-sector awareness programs, identified who is delivering them, and outlined delivery methods. Finally, the presentation included a gap analysis, highlighting efforts that the PCIS could encourage or take action on. The working group plans to move forward by:

- building a "living" repository of outreach activities that itself can provide wider access to and knowledge of awareness activities;
- implement a program specifically to improve awareness of the Partnership;
- develop metrics for effectiveness for key audiences; and
- identify additional programs to address "gaps."

6. Research & Development. The Federal Government has allocated $650 million to critical infrastructure security research, and several companies have robust research and development programs. Universities and other academic institutions are also conducting research in improving network security. However, there is no clearinghouse or mechanism to coordinate all these efforts. In July, working group #4 delivered a preliminary report on priority R&D topics. The PCIS will undertake to develop a full "CIP Research and Development Roadmap," to recommend to industry where to focus its efforts and to help government avoid duplication of effort.

7. International collaboration. This is not a US-only problem. Much of industry operates and delivers services and products on a global scale. The industry participants of the PCIS believe that the international dimension of critical infrastructure security has not been adequately addressed to date. The PCIS will actively engage in international outreach, to encourage

countries and nation unions to develop similar partnerships and to share information regarding threats, vulnerabilities, countermeasures, and best practices. We invite their attendance at our meetings, and would very much like to be kept informed of similar efforts elsewhere.

In the Internet Economy, no country or company can completely define its perimeter, and therefore we are all in this together. Working together, we can raise the bar of security worldwide, empowering the Internet generation as we move into the Internet century.

Partnership for Critical Infrastructure Security
Working Group 3
Public Policy White Paper

Executive Summary

- This working paper examines legal issues and challenges associated with cyber security risk management activities in the context of building a public policy framework to support these activities.

- There are several key assumptions underlying this framework: (1) that public-private partnerships are essential to meet challenges posed by new technologies and non-traditional threats; (2) that 20th-century government command-control policy frameworks and attitudes toward industry cooperation need to be adapted and modified to facilitate this partnership; and (3) that both the public and the private sectors have to walk a fine line in balancing security, commercial and public interests.

- The foundation of U.S. public policy should be to pursue the following: (1) establish guidelines for voluntary private sector information sharing with the government and within industry that address FOIA, anti-trust, and liability concerns. (2) establish guidelines for private sector cooperation with law enforcement that balance commercial and security interests. (3) Work toward fostering minimum global standards for law enforcement and private sector cooperation and toward establishing international conventions on critical infrastructure protection taking into account local cultural and social differences.

- At the international level, the Working Group suggests that the next Administration will have to walk a fine line between creating minimum levels of cooperation to enhance law enforcement and standards that try to impose government command and control models as opposed to models that enhance public-private cooperation. In addition, it would be very useful to develop a model template of security protections and civil measures, particularly for countries in Asia and Latin America currently lacking systematic approaches to the problem of e-security and critical infrastructure protection.

- Future issues to be addressed include: safeguarding trade secret protections, tax issues and incentives, simplifying industry-government agency relationships, clarifying government roles and responsibilities vis-à-vis industry, and identifying state and international legal and public policy issues.

Partnership for Critical Infrastructure Security

Legal and Public Policy Challenges for Critical Infrastructure Protection

White Paper

Table of Contents

Partnership for Critical Infrastructure Security

Legal and Public Policy Challenges for Critical Infrastructure Protection

White Paper

Introduction

This working paper examines legal issues and challenges associated with cyber security risk management activities in the context of building a public policy framework to support these activities.

There are several key assumptions underlying this framework: (1) that public-private partnerships are essential to meet challenges posed by new technologies and non-traditional threats; (2) that 20th-century government command-control policy frameworks and attitudes toward industry cooperation need to be adapted and modified to facilitate this partnership; and (3) that both the public and the private sectors have to walk a fine line in balancing security, commercial and public interests.

The United States currently operates under a public policy framework that is gradually shifting in response to the changed nature of economic security. However, many of the vestiges of twentieth century security structures and approaches still remain. While the U.S. is very well suited to handle conventional assaults, and has developed sophisticated strategies to deal with a wide range of military threats, more emphasis needs to be placed on integrating economic security measures into its strategic thinking.

The U.S. today is characterized by interdependence – government and industry have interwoven and entwined interests, to the point where it is estimated that almost 90% of the country's critical infrastructure is owned or administered by the private sector. As we enter the new millennium, cyber-terrorism, computer intrusions, and insider threats – whether through malicious acts or benign neglect -- may all contribute to a critical and costly problem for the U.S. business community, and by extension, to the U.S.'s economic sustainability and critical infrastructure security.

To ensure that America's critical infrastructures are protected, the government must work closely with the private sector. In the past, this was simply a question of setting up a command-and-control structure, but there are several reasons why this framework needs to be changed. First, there is a question of resources. By pooling resources, the government can leverage private sector assets, while at the same time, individual companies can tap into larger resources to better safeguard their private interests as well.

Second, there is a fundamental trade-off in economic security. Critical infrastructure protection has to be looked at, not just in terms of security, but in terms of its impact on commerce and trade as well (it goes without saying that there is also a fundamental link with civil liberties). The government should develop cost-benefit tests to determine whether a tool like the FBI "Carnivore" program is invasive/valuable. This requires a nuanced and "political" approach to the issue, and the optimal way to achieve

these benefits is by adopting a consultative approach before such tools are developed and implemented.

Third, partnerships represent a strategic choice for both the government and its private sector partners – voluntary commitments place less regulatory burdens but require more trust and openness.

Finally, there is the nature of the threat environment in a networked community. Threats and incidents can happen to anyone at any time in seemingly random patterns. If only for this reason, the ability to gather input from many sources is important.

However, to encourage private sector entities to voluntarily work with government, and to cooperate amongst themselves, protections and incentives must be given to businesses. Government agencies must recognize that while the private sector collectively may have access to vast resources, individually companies have finite resources and have fiduciary obligations to their stockholders that may constrain their public involvement. To the extent that government agencies can incentivize cooperation, reduce regulatory and security burdens, the greater the ability will be for individual companies to participate in security partnerships.

In discussions with elected officials and government agencies, the business community must be able to articulate what barriers exist that could hinder the private sector's ability to manage risks associated with cyber security – many of which are not fully understood, but all of which may result in substantial harm and liability to the commercial sector.

It is also important that security partnerships be attractive to all of the critical infrastructure industries and be inclusive rather than exclusive. In this regard, government agencies should be cognizant that different industries face different constraints and different threats and should work to make partnership models as attractive as possible for all of the critical infrastructure industries.

As Metcalfe's Law states: *the value of a network grows by the square of the size of the network*. So a network that is twice as large will be four times as valuable because there are four times as many things that can be done due to the larger number of interconnections. It is on the basis of this understanding that this public policy analysis seeks to enhance the power, and the potential, of the partnership model.

That being said, this White Paper is a work in progress. It is designed to serve as a basis for discussion for the development of public policy to enhance public-private cooperation and critical infrastructure security.

I. FOIA - Impediments to Sharing Information With the Government

Under the Freedom of Information Act ("FOIA"), there is a presumption that records in the possession of agencies and departments of the executive branch of the U.S. Government are accessible to the people. Recognizing the legitimate need to restrict disclosure of some information, and to promote cooperation with statutes and regulations, however, Congress has provided for numerous exemptions under which information is not subject to disclosure.

At present, it is not clear that any of the existing FOIA exemptions would provide the certainty of protection that many companies would require before believing that they could safely disclose threat and vulnerability information to the government. The Davis-Moran Act, currently being considered by Congress, would provide some level of protection for private sector companies that voluntarily provide cyber-security information to the government under certain circumstances. It is uncertain whether this legislation will pass.

Recommendation: Companies need to consider the FOIA issue as they work together to develop coherent and workable policies to encourage the voluntary disclosure of threat and vulnerability information to the government.

Hypothetical

The financial services industry is alerted to a pattern of internet-based attacks in which small amounts of money are wired out of numerous customer accounts and transferred overseas, where it becomes unrecoverable. In all cases, the banks have restored the funds to the customer accounts, so no individual customers were harmed; nevertheless, the reputational harm that could be caused has led to many institutions being apprehensive about their own vulnerabilities being disclosed to the general public.

Consider the case of three National Banks, Alpha Bank, Bravo Bank and Charlie Bank, who perform risk assessments, and learn of vulnerabilities to their systems under which such an attack could take place. While the type of threats, and resulting vulnerabilities are similar, the information is disclosed to the government under three very different scenarios.

Several of the Federal banking regulators, including the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision, and the Federal Reserve, have asked their regulated institutions for information about these threats to help in the Federal government's analysis of this activity. A consumer watchdog group that focuses on careless banking practices – ALERT -- learns of the losses, and files a FOIA request to make the information gathered by the agencies public.

For these examples, assume that The Davis-Moran Act has been signed into law, so there is a specific FOIA exemption for information about cyber threats voluntarily disclosed pursuant to a government request.

- Alpha Bank voluntarily shares information about a discovered software threat with the Office of the Comptroller of the Currency. Based upon Davis-Moran, the relevant agency FOIA administrator notes that the information was disclosed pursuant to a specific agency request, and *automatically* excludes Alpha Bank's disclosure from ALERT'S FOIA request without the need for further inquiry.

- Bravo Bank's software vulnerability information is inadvertently disclosed to the OCC while bank inspectors are reviewing Bravo's practices to ensure compliance with existing regulations. When ALERT's FOIA request is presented to the OCC FOIA administrator, Bravo Bank's disclosure does not fall within the Davis-Moran automatic exemption, and is not otherwise exempt under recent case law on the topic. The information is released to ALERT, which posts Bravo Bank on its "risky banks" web page.

- Charlie Bank discloses their vulnerability information at an industry conference on electronic banking. An OCC employee is present, and the information is put in a report and given to the division contemplating agency action. Charlie Bank's disclosure is not within the Davis-Moran exemption, and is not otherwise exempt under FOIA law and practice, so its vulnerability information is also released to ALERT and posted on the consumer watchdog's web page.

* * *

Companies should be advised that these are conceivable scenarios and should take suitable notice. As shown by these examples, there may not be sufficient protection currently offered to private-sector entities that disclose threat and vulnerability information to the government. Unless the Partnership acts to improve industry confidence, it is likely that some companies may view government requests for such information with a wary eye. Thus, changes to FOIA may be needed to remove private sector concerns about sharing information on critical infrastructure threats.

References:

Current Legislative proposals

H.R. 4246, Cyber Security Information Act 2000/Davis-Moran legislation

Examples of laws passed

1998 Y2K Information and Readiness Disclosure Act

Over eighty FOIA Exemptions throughout body of US law (e.g., filing patent application; submitting census information; filing IRS tax returns).

Financial Institutions, Suspicious Activity Report (SAR) form (covers financial institutions regulated by the Department of Treasury (OCC and OTS), Federal Deposit Insurance Corporation, Federal Reserve, National Credit Union Administration).

Legislative Next Steps

House Government Reform Subcommittee on Government Management, Information and Technology markup

II. Antitrust – Cyber Security Cooperation and Related Activities

Businesses need protection from unnecessary restrictions placed by Federal and state antitrust laws on critical information sharing. However, antitrust concerns reach beyond information sharing and encompass the full range of security cooperation strategies.

Neither the Department of Justice nor the Federal Trade Commission has embraced the need to develop voluntary guidelines for cyber security cooperation – similar to the guidelines the Federal government developed covering the health care industry.

Regardless of whether Davis-Moran passes, the PCIS would benefit from outlining an antitrust strategy that permits full and robust cooperation on security issues. Efforts within the administration might focus on both the FTC and DOJ staff responsible for recent guideline development (see, e.g., Antitrust Guidelines for the Licensing of Intellectual Property – (http://www.usdoj.gov/atr/public/guidelines/ipguide.htm). A similar state-based strategy may be necessary to preclude prosecution within the states.

Awareness and dialogue on security cooperation is an essential ingredient for managing legal risk associated with security cooperation. A PCIS antitrust strategy cuts across all sectors and works to limit liability in this important area.

Recommendation: Companies should inquire with the FTC and DOJ about guideline development for cyber security cooperation.

Recommendation: Companies should be aware that antitrust concerns reach beyond information sharing and encompass the full range of security cooperation strategies.

Hypothetical

Security officials from twelve petroleum companies, representing 80 percent of the industry, are meeting to form an ISAC. Possible security cooperation includes:

- Sharing of threat and vulnerability information, discussing and disseminating industry standards and practices, and sharing other relevant data;
- Using ISAC data to perform research and development activities in the cyber security area, and/or
- Licensing software products, developed by the ISAC with industry data, to identify threats peculiar to the petroleum sector.

* * *

This example is intended to highlight three distinct areas of security cooperation that may lead to antitrust liability. Federal antitrust law and policy is concerned with furthering competition in the marketplace. Certain types of agreements, cooperative arrangements, and information sharing amongst industry participants may have anticompetitive effects. This is especially the case where the agreements (or, collaborative models) have the effect of raising prices or reducing outputs – irrespective of intent.

Thus, even though the ISAC participants in the hypothetical do not intend to violate antitrust law, both the Federal Trade Commission and the Department of Justice, as the government's lead agencies for antitrust enforcement, may bring an action against the industry participants.

Both the Department of Justice and the Federal Trade Commission understand that cooperation may actually further competition and make good business sense. As a result, both agencies have carefully developed and issued several Statements of Antitrust Enforcement Policy ("Joint Antitrust Statements"), clarifying issues of cooperation among competitors. Published statements include:

- Licensing of Intellectual Property;
- Health Care Joint Ventures and Mergers;
- Collaborations Among Competitors; and
- Joint Venture Relationships – including international partners and corporations.

The Joint Antitrust Statements explicitly spell out what types of ventures, agreements, and activities fall within a "safety zone" of acceptable activities, as well as what activities are *per se* illegal; the Joint Antitrust Statements additionally provide a "rule of reason" analysis for those otherwise falling outside the safety zone.

From the PCIS perspective, we are discussing cooperation among competitors in high profile and politically charged industries, such as petroleum companies, Internet Service Providers, financial services, and insurance. The mere cooperation of large segments of various markets may raise questions by non-participating members in relevant markets, regulators, consumer organizations, and a variety of other political actors, candidates, agencies, and non-government organizations – thus increasing the risk of participation.

Although it is possible, and perhaps even likely, that DOJ/FTC analysis of security-related cooperation would ultimately be found to have a legitimate purpose, and not foster anticompetitive effects, the better course of action might be for the PCIS to consider fully the range of potential antitrust liability, and to seek guidance and statements of policy from DOJ/FTC. These statements will work to limit and manage risk associated with cooperation activities.

There are, of course, models that the PCIS may utilize in discussions with relevant agencies and regulators. For example, most critical infrastructure protection programs

will have a major R&D component. The question arises whether there is some language or provision that can be borrowed to serve as a model. There are several industry cooperation models operating under legislative provisions currently in place such as the National Center for Manufacturing Sciences and the Semi-Conductor Research Corporation, so that the private sector does have meaningful experience that can be applied. The U.S. Government has already developed antitrust policy on research and development activities, on IP licensing, and on joint ventures – and these models may easily be applied to PCIS activities as well.

Recommendation: Corporate representatives should explore existing models of legislation and apply past experience and lessons learned from these models to new CIP issues.

References:

Current Legislative proposals

H.R. 4246, Cyber Security Information Act 2000

Examples of laws passed

1998 Y2K Information and Readiness Disclosure Act

U.S. Dep't of Justice, Justice Department Merger Guidelines, 49 Fed. Reg. 26,823 (1984), *reprinted in* 2 Trade Reg. Rep. (CCH) No. 655 PP4490-4495 (June 18, 1984).

1984 National Cooperative Research Act; 15 U.S.C. 4301.

III. Liability – Managing Risk for Owners/Operators of Infrastructures

Businesses need to be shielded from legal liability for a wide range of risk management planning activity – such as performing risk assessments, testing infrastructure security, or sharing certain threat and vulnerability information.

The PCIS should carefully and comprehensively consider liability concerns from commercial, technological, and legal perspectives. The PCIS should use the Interdependency Vulnerability Assessment Working Group's findings as it determines how to prioritize immediate/current risk concerns in terms of how they should be approached in the public policy arena. Liability issues and solution sets should complement PCIS efforts in other working groups and operate across all critical infrastructure sectors.

Current concerns for liability reach well beyond information sharing – which largely defined the legal concerns for the past two years. Information sharing is a foundation issue for the PCIS, and thus liability resulting from the sharing of threat and vulnerability information is very real. There are, however, broader, and perhaps weightier liability concerns that are of immediate commercial importance.

Recommendation: Businesses should be aware that issues to be addressed in this field include:

- Defining state-based duties of care for corporate senior management as well as directors/officers.
- Analyzing the impact of the recently released Gramm-Leach-Bliley cyber-security regulations and discussing whether the PCIS should comment on the agencies' implementation plans – especially since coverage will include entities beyond the financial services community.
- Discussing vendor-management legal issues, including whether/how due diligence models are possible to implement in the Information Age.
- Analyzing whether damages should be capped for downstream harm resulting from cascading impact. This may be an appropriate area for Federal preemption.
- Identifying appropriate roles for Federal and state government to limit liability for owners/operators of critical infrastructure facilities.
- Developing an understanding of the insurance industry and working to facilitate strategies that support cyber-security/liability insurance availability across all sectors; and
- Liability that might arise due to inconsistent state and national laws that place inconsistent requirements on national or global companies.

Hypothetical

Congress, worried about the release of corporate proprietary data and customer personal information, passes a statute requiring Federal regulators to establish Federal cyber-security guidelines. Significant portions of these guidelines focus on the importance of performing a risk-assessment analysis and on involving senior management and directors in all significant information-security decisions. The regulators mandate that cyber security cover technical, physical, and administrative areas.

Company Alpha, which provides telecommunications-related services, and stores significant amounts of non-public customer data, performs a thorough risk assessment. Company Alpha reviews a range of threats and vulnerabilities by involving company representatives from each of the major service centers and technology offices, involving both its internal and external auditors in the review. Company Alpha subsequently fixes a vast majority of the discovered gaps and security issues.

Company Alpha chooses, however, not to fix a small number of the discovered security vulnerabilities:

- Senior management reports these decisions to the CEO and Board of Directors. The Directors query senior management on their decisions, which are based on the high cost of fixing these problems, the low-risk assessment given them by the audit committee reports, and a belief that the problems can be easily managed and with compensating control.
- A shared belief exists amongst management and the audit committee that these low-level risks are not likely to undermine delivery of services essential to the business or result in the loss of customer data; general counsel agrees that the risk is not significantly large to warrant the added security costs.
- The audit committee, working closely with senior management, the Chief Technology Officer, and a newly appointed Chief Information Security Officer, prepare a written information security plan, which includes a component on managing the low-risk vulnerabilities, taking into account technological solutions and employee practices.

In contrast, Company Bravo chooses not to perform a comprehensive risk assessment focused on consumer non-public privacy data. Internal and external auditors do not involve senior management, nor is the CEO or Board of Directors involved in any of the Company's information security activities.

Both companies experience an "insider" problem, resulting in the release of personally identifiable customer information. The New York Times reports on the release of customer data at both companies, leading to a massive drop in stock prices at both Companies Alpha and Bravo. The Trial Bar celebrates as word is out on the first information-security shareholder derivative lawsuits.

* * *

The PCIS might consider addressing duty of care and standard of care issues relating to commercial information security matters. This hypothetical focuses on standards of care to protect non-public customer or privacy data – irrespective of the company's business model or service-delivery practices.

The Davis-Moran legislation, now being debated by Congress, focuses on liability resulting from information-sharing practices, but the exemption from liability is only for information-security disclosures made under certain highly defined situations involving information provided to the government.

Recommendation: Corporate representatives should consider several issues:

- Should the PCIS promote exploration of the full range of legal liability issues?
- If the PCIS, or other organizations, do not raise and move these issues forward, what is the possible harm (Court decisions will establish standards? State lawmakers will provide input into decision-making process, *etc.*?)
- If the PCIS is going to explore liability issues, what are the priorities?
- How should the PCIS identify and support industry standards and duties of care?
- Additionally, should the PCIS identify strategies to raise awareness and/or to effect political/legal change in this complex area?

References:

Current Legislative proposals

H.R. 4246, Cyber Security Information Act 2000

Examples of laws passed

1998 Y2K Information and Readiness Disclosure Act

IV. Encryption

On July 17, the Administration announced a substantial further relaxation on export controls on encryption as controlled by the latest policy effective on January 14. For a summary and links to the press release, fact sheet, and text, go to http://207.96.11.93/Encryption/Default.htm.

The January policy's significance was that licensing applications would often draw positive answers where they would have been declined before. At the same time, cumbersome existing rules and procedures largely remained in place. The European Union, however, forced a prompt reconsideration of the January policy with its decision to allow encryption exports within the EU and selected other leading countries on a license-free basis, once again putting U.S. suppliers at a significant competitive disadvantage. The October policy has the effect of removing that major advantage by allowing U.S. encryption exports on a license-free basis to the EU and eight other countries. The upshot is that, for global security solutions, U.S. firms across the board, as licensees, can now rely on U.S. vendors as well as foreign vendors. Previously, foreign systems integrators and IT vendors enjoyed a legal advantage in serving global customers, whether based outside or inside the U.S.

On October 2, Commerce Secretary Norman Mineta announced that the Department of Commerce had selected a new encryption algorithm to become a federal procurement standard. The 23-year old, 56-bit Data Encryption Standard (DES) will be succeeded as Federal Information Processing Standard (FIPS) by "Rijndael," a 256-bit algorithm submitted by two Belgian programmers who -- as IBM had done with DES -- dedicated the formula to the public domain, making no patent claims. The announcement (http://www.nist.gov/public_affairs/releases/g00-176.htm) caps a three-year search; a formal 90-day comment period will be announced soon in the *Federal Register*. Replacement of DES has become increasingly urgent, as it presents intruders with only a constant level of difficulty in penetration, in the face of processing power available to intruders advancing in accordance with Moore's Law of price-performance doubling every 18 to 24 months. The arrival of a replacement for DES is good news for all firms desiring to ratchet up their level of protection.

Both major policy developments, long in the making, largely coincide with the inception of a new Administration, thus affording the best opportunity in years to move past previous rancorous episodes in computer security issues. If government shows appreciation of the need for consultation, rather than presenting the private sector with a *fait accompli*, and industry demonstrates an appreciation of the common dangers confronting it along with government, then a fresh start is possible.

V. Cost Recovery

How will the cyberthreat defensive expenditures of U.S. firms be treated for federal corporate income tax purposes? In particular, will firms be allowed to expense these amounts or will they be required to amortize them, even if firms do not want to do so?

To the extent that firms can expense such expenditures, they are more able to undertake them. This is especially true if, in some circumstances, government authorities would have some reason for wanting a firm in question to erect higher defenses than the firm's management or board thought its fiduciary responsibilities called for. If the government wants increased cyberthreat expenditures by industry, presumably favorable rather than adverse tax treatment would be part of a larger government policy toward that end.

Nonetheless, in the last decade the Internal Revenue Service has taken an aggressive position on the expensing vs. depreciation issue. Emboldened by its success before the Supreme Court in the 1992 *INDOPCO* case, the IRS now calls for companies to amortize certain expenditures over time even when the taxpaying firm wants to expense them in one year and be done with it. The Supreme Court ruled that a target company could not deduct the costs associated with a friendly takeover by another company because the merger would lead to future benefits for the target company. Since then, the IRS has been very aggressive in applying this decision to a wide range of costs incurred by businesses. In general, the IRS takes the position that any cost that results in a future benefit to a business must be capitalized, rather than deducted currently. The IRS uses a broad definition of "future benefit" and, in many cases, has required companies to capitalize costs that they have been deducting for years. At this point, the service has applied INDOPCO to a wide range of costs incurred by businesses, including the costs related to customer acquisition, contract bidding, post-merger severance, business expansion, redoing software, equipment inspection, plant closings, equipment moving, environmental remediation and equipment removal.

Recent favorable developments are the IRS's interpretations that firms' expenditures to meet ISO 9000 quality standards and to achieve Y2K compatibility may be expensed. To the extent that firms are moving to meet recognized standards in the computer security area, then the ISO 9000 interpretation perhaps could serve as a precedent. The PCIS notes both the potential upside and the potential downside in the tax treatment area and recognizes that structuring an appropriate tax policy to incentivize the reduction of the national vulnerability to cyberthreats is an integral part of the emerging public policy framework that needs to be developed.

VI. Economic Espionage and Trade Secrets

A major motivation of commercial cyber security is the protection of a firm's trade secrets. While one can assign no precise value, about 75% of the roughly $10 trillion capitalization of today's publicly traded companies represents the "enterprise value" or increment above book value assigned to intangibles – business model, management and workforce strength, and intellectual property portfolio.

Four years ago, Congress passed the first-ever federal protection for trade secrets in the marketplace with the Economic Espionage Act (EEA; P.L. 104-294), following testimony by FBI Director Freeh that 23 countries had targeted the U.S. to steal the trade secrets of leading U.S. firms. Estimates of the annual loss run to $250 or $300 billion. The law contains harsh penalties and has been used sparingly.

The Trade Secrets Act (18 U.S.C. 1905), a much older part of the criminal code, makes it a crime for a federal employee to divulge a trade secret entrusted to that agency. At the same time, years of litigation under the Freedom of Information Act – under which one company has often sought to learn more about its competitor – have left a situation in which the case law suggests that cyber trouble reports to the government will not be released. That result, however, is not spelled out in black and white.

An attack or attempted penetration of a corporate computer system may be hard to characterize at first. Is it of domestic or foreign origin? Initially, one cannot tell; hence the serious prison penalties in the EEA, which, while aimed at foreign agents, apply equally to all offenders. Does the attacker intend to disrupt systems or to purloin files? Again, this will not be immediately obvious.

Corporate MIS, CIO, or chief security officers are working off a base of protection of highly valuable corporate secrets that lend a competitive advantage against espionage intended to purloin rather than to disrupt. Defending against deliberate disruption represents a new challenge, but presumably many of the same tools and methods will continue to apply.

Data about attacks or attempted penetrations do not represent a trade secret in any traditional sense, as they do not lend any kind of competitive advantage. To the contrary, cyber vulnerabilities, to extent they are not widely shared – which in some cases they will be – represent a competitive *disadvantage*.

At the moment, companies can divulge trade secrets to the government with greater confidence than trouble reports. Increasing the confidence of companies that trouble reports will not be made public under the Freedom of Information Act is what the Cyber Security Information Act, H.R. 4246 (Davis-Moran), is largely about.

VII. International Issues

Goals:

- Facilitate international law enforcement cooperation
- Establish minimum standards for cyber-security legislation taking into account local cultural and social differences.
- Move away from command-control concepts to expanding partnership opportunities.

At this time, the priority from an international public policy standpoint should be to establish a collaborative international regime that facilitates law enforcement cooperation, establishes a balance between commercial and security interests, and facilitates international public-private partnership.

In this view, the chief threats to economic security are sub-national terrorist groups, criminal organizations, mischief-makers and hackers. This is not to say that the U.S. should be blind to state-sponsored threats, and companies are well advised not to assume that their technologies cannot be targeted by state agents. However, all nations have a vested interest in working together to mitigate the damage caused by terrorism, crime, and mischief.

Currently, there are – broadly speaking – four different cases that need to be managed: (1) cooperation with developed countries, perhaps best captured through the framework of the OECD; (2) cooperation with emerging countries such as Brazil and the Philippines; (3) cooperation with communist and post-communist states; and (4) containment of what were formerly known as "rogue" states.

In the first case, there are a number of initiatives already underway. Perhaps the most significant of which is the Council of Europe's Draft Convention on Cybercrime.

On October 2, the Council of Europe released Version No. 22, Revision 2, of its Draft Convention on Cyber-crime, which would grant police much greater powers to access electronic information. The convention is an attempt to standardize computer crime statutes throughout Europe, and require signatories to cooperate with one another. The Council of Europe is pushing for the Convention to be agreed to by December.

The convention proposes among other things that countries adopt laws criminalizing unauthorized computer access or data interception or manipulation, as well as the possession of passwords or other common security tools if they are held with the intent to commit an offense. It also proposes laws to enable government access to encrypted information and to expand copyright protections.

(The Council of Europe "Draft Convention on Cyber-crime" is open for public comment (email: ***DAJ@COE.INT***))

However, a coalition of 28 prominent international cyber-rights organizations have come out against the current draft, stating that it could result in outlawing network security tools and would require companies to review and keep extensive logs of the message traffic on their systems. In a letter sent to the Council of Europe Secretary General, the Global Internet Liberty Campaign, which includes prominent groups from the U.S., France, Britain, Australia, Bulgaria, Canada, Italy, South Africa, Austria, the Netherlands, and Denmark, claims the treaty is little more than a law enforcement wish list. Industry has expressed similar and additional concerns related to the regulatory burden and cost of certain proposed measures. Industry representatives should advise the next U.S. government about these problems, and encourage the next government to work with the Council of Europe and the OECD to revise their current policy and move toward a more "partnership" oriented model.

The second and third cases – creating cooperative models with communist and post-communist countries and with developing countries can be treated in relatively similar fashion. In these cases, the U.S. may wish to propose basic legal formulas for treating cybercrime and establish basic ground rules for law enforcement cooperation. These formulas should be flexible and take into account social and cultural differences.

Companies should be aware that countries like Brazil, Mexico, India, the Philippines, China, and Russia have developed significant computer and technically literate populations, and either do not currently have cybercrime legislation, do not have comprehensive legislation, or do not have adequate enforcement and remedy provisions.

This is important to bear in mind, considering that the Philippine student who allegedly unleashed the "I Love You" virus did not break any cybercrime laws.

Creating a global consensus to promote the benefits of cooperating to safeguard network systems and to facilitate state-state, public-private cooperation will enhance economic stability and have other commercial and political benefits.

In the fourth case – dealing with countries such as Cuba, Iran, Iraq, and North Korea – cybersecurity discussions should be integrated into other ongoing diplomatic discussions as part of the overall set of issues involved in relations with these states.

VIII. Attachments

There are various other matters that require immediate examination and thought. As a result, attached to this White Paper are several support documents, including:

- A listing of legislative initiatives that were considered by the U.S. House of Representatives and Senate in the Fall of 2000 (Attachment 1);
- A listing of additional legal issues (Attachment 2);
- A listing of a set of principles for voluntary information sharing (Attachment 3);
- A summary of an Amendment offered by Senator Bennett to require the Defense Department to clearly define its contribution to critical infrastructure issues – both public and private sector related (Attachment 4);
- A summary of the Cyber Security Information Act, H.R. 4246 (Attachment 5); and
- A summary of the Interagency Security Guidelines published pursuant to the Gramm-Leach–Bliley Act (Attachment 6).
- Select legal definitions (Attachment 7).

Attachment 1

2000 House and Senate Legislative Proposals

In addition to HR4246 (Attachment 5), the following are a list of other measures under consideration by the House of Representatives and the Senate that could affect the public policy framework governing critical infrastructure protection. The variety of legislative proposals reflect different strands of current U.S. strategic thinking vis-à-vis critical infrastructure protection and the range and complexity of issues that need to be addressed.

Department of Defense Authorization Act (H.R. 4205) — "Bennett-Schumer" Amendment: Under this legislation the Department of Defense is:

- required to better define its role in, and explain to Congress its coordination with other governmental efforts related to, critical infrastructure and information system protection
- given $15 million to recruit cyberwarfare specialists
- given $5 million to create an Institute for Defense Computer Security and Information Protection
- authorized to provide loan guarantees to improve domestic preparedness to combat cyberterrorism.

H.R. 2413 — Computer Security Enhancement Act of 2000: H.R. 2413 would require the National Institute of Science and Technology (NIST) to serve as a computer security consultant for federal civilian agencies. NIST would offer the government guidance on protecting the security and privacy of sensitive information in agency computer systems. In this role, NIST would be encouraged to recommend "technology neutral" solutions to security problems, and to advise government agencies on which "off-the-shelf" computer security products met with the government's standards. H.R. 2413 also would require NIST to study the effectiveness of commercially available encryption products.

H.R. 4987 — Digital Privacy Act of 2000: Would ease law-enforcement monitoring of electronic communications.

H.R. 5018 — Electronic Communications Privacy Act of 2000: As substantially revised, H.R. 5018 is primarily focused on privacy concerns raised in reaction to the FBI's "Carnivore" e-mail surveillance program. Because it is vastly different from the primary Senate-passed cybercrime bill (S. 2448, below), no further action is likely at this late date in the legislative year.

Senate Bills

S. 1314 — Computer Crime Enforcement Act: S. 1314 would authorize $25 million for the Department of Justice to help states develop computer crime enforcement units.

S. 1993 (Government Information Security Act): Attempts to strengthen federal information security practices and coordinate government information security efforts with those of the civilian, security, and law enforcement communities.

S. 2430 (Internet Security Act of 2000): Broadens the scope of the existing $5,000-loss minimum required to permit federal jurisdiction over computer hacking cases, permits forfeiture of property used in computer hacking crimes, increases the availability of law-enforcement wiretapping, and eliminates mandatory minimum sentences for certain computer hacking crimes.

S. 2448 — Internet Integrity and Critical Infrastructure Protection Act of 2000: As amended, S. 2448 would, among other things, give the Secret Service jurisdiction to investigate certain computer crimes, including those against financial institutions, increase penalties for criminal activity that used encryption; authorize $5 million to establish a Deputy Assistant Attorney General to oversee the Justice Department's Computer Crime and Intellectual Property Section, and give DoJ $80 million to create 10 regional computer forensic labs that would provide education, training, and forensic capabilities to state and local law enforcement charged with investigating computer crimes, and another $20 million to establish a National Cyber Crime Technical Support Center. The bill would also permit the confiscation of equipment used to commit computer crimes, allow the prosecution of juveniles, increase various computer-crime penalties to as much as 20 years in prison, and would require the U.S. Sentencing Commission to review and perhaps revise the sentencing guidelines for computer crimes, including elimination of the six-month mandatory minimum sentence for reckless crimes.

S. 2451: Creates a National Commission on Cybersecurity, increases penalties for certain computer crimes, and broadens the applicability of those penalties.

S. 3188 — Cyber Security Enhancement Act: S. 3188 would call for more protection for U.S. critical infrastructure from hackers, terrorists and rogue nations by allowing companies to voluntarily submit information that the government would not otherwise have about weaknesses in their online systems, as well as information on threats and attacks to the federal government, without fearing that the information would be subject to disclosure under the Freedom of Information Act. In addition, S. 3188 would permit the Attorney General to issue administrative subpoenas to trace cyberattacks, and would require the A.G. to report to Congress on plans to standardize information requests to business, and efforts to encourage the technological prevention of falsifying e-mail addresses.

Attachment 2

Additional Issues for Future Consideration

- State Legal and Public Policy Issues

Current and prospective state laws should be reviewed and assessed. The extent to which such laws would be preempted by federal law should also be assessed.

- Simplifying and Clarifying Industry-Government Relations

Industry is working with a number of different government agencies on CIP issues. These relationships should be mapped out, and this may facilitate public-private engagement and streamlining practices.

- Federal Regulations

Proposed federal regulations should not be issued without first evaluating their impact on critical infrastructure, akin to an Environmental Impact Statement, and should not be finalized without attempting to mitigate any adverse effect. There are now several pending rulemakings that have serious adverse impacts on critical infrastructure providers, and there is no federal policy which requires those impacts even to be considered, much less appropriately accommodated.

- The Impact of Privacy on Security Issues

- Public and Private Access

Attachment 3

Initial Set of Principles for Voluntary Information Sharing

- Existing laws should be adapted as necessary to allow appropriate levels of voluntary information sharing among companies, and between the private sector and government.

- Industry should continue to monitor the private sector portion of the Nation's critical infrastructure and should cooperate both internally and with government in reporting and exchanging information, as appropriate, concerning threats, attacks, and protective and recovery measures. Coordination among principals must facilitate creation of responsible activities ranging from early warning systems to response, restoration, and recovery initiatives.

- The creation and operation of voluntary information-sharing mechanisms or processes should not expose participants to additional regulatory or other proximate liability. Private industry efforts to avoid or reduce cyber-threats and other harm to critical infrastructure should be given regulatory "safe-harbor" status, and should be favored under the law at least as much as "Good Samaritan" efforts.

- Distinctions should be made among cyber-mischief; cyber-crime and cyber-war to clarify jurisdictional issues and determine appropriate responses. The adequacy of current laws to prevent these threats must be reviewed. As necessary, existing laws should be adapted to take these matters into account.

Attachment 4

Summary of Bennett Amendment

- On June 20, the Senate unanimously approved Bennett-Schumer, which requires the Department of Defense, and all other agencies to report to Congress on plans and programs to organize and coordinate defense against attacks on critical infrastructures and critical information systems in both the public and private sectors.

- The legislation is principally aimed at requiring the Defense Department to define its role in PDD-63 activities. Specific requirements include:

    - Identifying the necessary definitions of a "nationally significant cyber-event" and "cyber-reconstitution";

    - Describing how the Defense Department is working within the Intelligence Community to identify, detect and counter the threat of information warfare of foreign states and transnational organizations; and

    - Explaining how the Defense Department is integrating the National Communications Systems and the Joint Task Force/Computer Network Defense into an Indications and Warning architecture.

- The proposed legislation also requires the President to submit a report to Congress by July 2001 detailing the specific steps the Federal government has taken to develop infrastructure assurance strategies, as outlined in PDD-63.

- The bill was accepted unanimously as an amendment to the Department of Defense Authorization Act, which is currently pending in the Senate.

- Keep in mind that the bill does not relate to the Computer Security Act of 1987, and the repeal of National Security Decision Directive 145, which dealt with authority to create minimum computer security standards and guidelines within the Federal government. Rather, the emphasis is wholly on identifying a clear role for the Defense Department in the on-going PDD-63 activities.

Attachment 5

Summary of "Cyber Security Information Act of 2000"

H.R. 4246, "The Cyber Security Information Act of 2000" introduced by Congressmen Tom Davis (R-VA) and Jim Moran (D-VA) accomplishes two major goals. First, it provides limited protection from unintended uses for cyber-security information voluntarily shared with the federal government. Second, it describes alternative mechanisms for sharing such information with the government.

As for the mechanisms for sharing cyber-security information with the government, the Act specifies that the government may ask for voluntary submittal, directly to the government, of detailed company-specific cyber-security information (as defined) in order to assess the cyber-security of an industry or economic sector. Further, the government may request that cyber-security data be submitted to a non-governmental entity that agrees to coordinate such data gathering and then pass on that information to the government, most likely by means of its own summary and assessment of the data. In addition, such non-governmental entity may obtain the benefits of this provision even if it performs those functions without first being asked by the government, as long as it does in fact provide such cyber-security data and/or analysis to the government.

Next, regarding the protections provided to cyber-security information , the Act stipulates that any and all cyber-security information (as defined) voluntarily provided to the government or aforesaid non-governmental entity will be given a broad immunity from forced release to any other entity or individual. This is accomplished in two ways. First, the Act specifies that all cyber-security information voluntarily provided to the government pursuant to this process is deemed to be exempted from disclosure under the Freedom of Information Act (FOIA). This exemption is similar to already-existing FOIA exemptions, such as those for trade secrets and national security, but would not be subject to the uncertainties, vagaries, and delay of case-by-case agency determination, along with any attendant litigation delays associated with making such case-by-case determinations. Moreover, to the extent that any such cyber-security data actually held by a third party could be said to be held by the government by virtue of that third party acting on behalf of the government, FOIA would still not require the release of such data.

Second, no entity may use any other means (such as a subpoena) to force the government or the third-party data-gatherer to yield up cyber-security data. However, to ensure that the government obtains the full use of any related or similar data that it receives, and that no injustice would be worked against a party to litigation, the Act further provides that cyber-security data can be used **(a)** by the government if obtained pursuant to some statutory or regulatory requirement (rather than voluntarily), or **(b)** by anyone for any purpose once the information has been made public with the permission of the originating entity. Moreover, a litigant may utilize any existing lawful means already available to it (such as a subpoena) to obtain such data directly from the originator.

Attachment 6

Summary of Gramm-Leach-Bliley Cyber-Security Provisions

- In November of 1999, Congress passed the Financial Services Modernization Act, referred to as the Gramm-Leach-Bliley Act ("G-L-B"), repealing Glass-Steagall and streamlining the financial services legislative and regulatory framework.

- In response to pressure from the privacy community, which was concerned about customer information being circulated within the newly opened financial services atmosphere, Congress included language in G-L-B to protect personal information in the possession of the financial services industry.

- Generally speaking, the statute mandates that various federal regulators "establish appropriate standards for the financial institutions subject to their jurisdiction" for identifying and protecting certain customer information (Refer to Sections 501 to 505 of the law):

  (1) To insure the security and confidentiality of customer records and information;

  (2) To protect against any anticipated threats or hazards to the security or integrity of such records; and

  (3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience of any customer.

- The law includes three distinct requirements: technical protection (cyber-security), administrative protection (social engineering policies), and physical security protection. (Collectively, "cyber-security"):

- Relevant agencies and department include: the Securities & Exchange Commission, Federal Deposit Insurance Corporation, Department of Treasury entities (OCC and the OTS), the Federal Reserve Board of Governors, and the National Credit Union Administration.

- Congress additionally requires state-based insurance regulators to issue similar standards for entities under their jurisdiction; failure to do so may result in curtailed federal funding, such as FDIC-provided insurance guarantees.

- In response to the statute, several of the listed agencies and departments cooperated to develop appropriate standards and guidance, forming the Financial Services Legal Working Group, which met during a six-month period to develop

a sophisticated collection of cyber-security guidance materials. The "Interagency Guidelines" were published in the Federal Register on June 26, 2000.

- The Interagency Guidelines establish several key responsibilities:
    - Involving the Board of Directors and Senior Management throughout the information security planning process;
    - Identifying threats and vulnerabilities to information and cyber systems;
    - Performing a risk assessment based on these threats and vulnerabilities;
    - Overseeing and carefully managing vendors that have access to customer data ("due diligence" standards); and
    - Implementing a written information security policy and program.
- In addition, the guidance materials require implementing various other due-diligence responsibilities, such as training staff, preparing emergency response programs and business contingency plans, and appointing a Chief Information Security Officer.
- While G-L-B is aimed at the financial services industry, the reach of the law is unclear; the Federal Trade Commission has jurisdiction to issue cyber-security guidelines for entities under its jurisdiction – which includes, in effect – anyone engaged in e-commerce. In addition, G-L-B applies explicitly to affiliates and service providers who maintain or process any of the targeted customer data.
- How these Interagency Guidelines will be used in litigation is also a significant issue. In particular, industry and government should monitor the extent to which the Interagency Guidelines establish a duty of care or industry standard, which may be relied on in litigation stemming from a cyber-intrusion or breach of confidential customer data.
- Comments must be received not later than August 25, 2000. Agencies will separately review the responses and publish final rules this fall. The statutory deadline is November 13, although agencies may choose to extend the deadline. Compliance is mandated by July 2001.
- One complex question is the extent to which the FTC will engage the cyber-security issue. The agency has always taken an aggressive approach to online privacy, and to the extent that security relates to privacy concerns, they, too, might issue their own regulations for a multitude of other industries. As mentioned, service providers that hold or process any of the personal information covered by the G-L-B are also subject to the regulations. This, too, may serve as a hook for the FTC – or another agency – to regulate cyber security issues. An

additional complexity is the extent to which state agencies will publish cyber-security guidelines.

- The SEC published its proposed rules on March 8, 2000 (65 Fed. Reg. 12354 (March 8, 2000)). (In sum, a *financial institution may be in compliance if it adopts measures to protect against reasonably anticipated threats and hazards*). The SEC has not developed, nor does it plan to prepare, any further regulations in this area. Similarly, the FTC has not prepared specific guidance or regulations in the security area.

- One other complex, unresolved issue is the extent to which the Interagency Guidelines will be enforced as regulations or left as voluntary guidelines by each department/agency. The regulators are seeking comment on these and other issues raised in the materials.

Attachment 7

Legal Definitions

Due Diligence. Actions expected from a reasonable and prudent person under particular circumstances. Such diligence is not measured by any absolute standard but depends upon the relative facts of a special case (see "Reasonable" below).

Duty of Care. An obligation to conform to a legal standard of reasonable conduct in light of apparent risk. In a negligence context, the word "duty" denotes the fact that the actor is required to conduct himself in a specific manner. If he does not, he becomes subject to liability to the party to whom the duty is owed for injuries resulting from the non-conforming conduct. For example, a corporate officer has a duty of care over corporate assets.

Limitation of Liability (Acts). State and federal statutes that limit liability for certain types of damages (lost profits, costs, etc.) or of certain groups or persons (liability of corporate officers for certain acts of the corporation). When used to limit damages, sometimes referred to as a "cap."

Precedent. An adjudged case or decision of a court, considered as furnishing an example or authority for an identical or similar case arising afterward or a similar question of law.

Preemption - Doctrine, adopted by the United States Supreme Court, holding that certain matters are of such national, as opposed to local, character that federal laws take precedence over state laws. In such a situation, a state may not pass a law inconsistent with the federal law.

Per se Illegal. "Per se" means: in itself; taken alone; inherently. In an antitrust context, certain types of business agreements, like price-fixing, are considered "per se" illegal because they are deemed to be inherently anti-competitive and injurious to the public. For those acts, courts do not examine whether there has been any actual damage from the activity. Liability is imposed simply because the act took place.

Reasonable – Fair, proper, just, moderate, suitable under the circumstances. For example, if two companies exchange information regarding infrastructure security, those actions would be judged based upon what other similarly situated companies would do in like circumstances.

Rule of Reason. Under the "rule of reason" test in antitrust cases, the legality of restraints on trade is determined by weighing all of the factors of the case, such as the history of the restraint, the evil alleged to exist, the reason for adopting a particular remedy and the purpose or end sought to be attained. The fact finder must weigh all the circumstances to decide whether a practice unreasonably restrains competition, and the test requires that a plaintiff show anti-competitive effects or actual harm to competition and not simply whether a given practice is "unfair."

Safe Harbor. Usually refers to a set of guidelines established so that companies can be protected from liability or regulation under a given law. For example, a statute might state that if a company takes actions "A", "B", and "C", then, depending on the statute, that company would either avoid liability, limit its potential liability or be exempt from regulation.

Trade Secret. A "trade secret" may consist of any formula, pattern, concept or device used in one's business which gives an advantage over competitors who do not know or use it. Trade Secrets are intellectual property, but do not necessarily have patent, trademark, or other formal intellectual property protection.